Cryptographic Engineering Research Group
Presents

ECE DEPARTMENTAL SEMINAR

Sources of Randomness in Digital Devices and Their Testability

Viktor Fischer, Ph.D.
Hubert Curien Laboratory
Jean Monnet University, Saint-Etienne, France

Wednesday, May 4, 2016
10:30-11:30am, ENGR 4801

Abstract:

Digital electronic devices are often used to implement data security systems-on-chip (SoC), like smart cards. Random bit stream generators constitute one of the main building blocks of such systems. They use some uncontrollable physical analog phenomenon as a source of randomness. The random variations in this analog process must be converted to a digital bit stream using some intrinsic analog to digital conversion or some extrinsic digitization technique. This conversion should be feasible using purely digital technology, because the use of some analog electronic blocks inside the device would increase the total cost of the system.

In this talk, we will shortly discuss physical analog phenomena that can be used as sources of randomness in digital devices, and analog to digital conversion techniques that can be exploited in this kind of devices to generate the raw random binary signal.

We will present the random physical processes existing in digital devices from the point of view of their possible quantification inside the device using embedded signal measurement techniques. The measurement process can serve as a basis for a fast and efficient dedicated statistical test, which can be embedded inside the same device. This test could complete or even replace continuous health tests required by the current version of the standard. However, instead of using the raw binary signal as required in the standard for the general-purpose continuous tests, the dedicated tests would use signals, which are closer to the physical source of randomness (they can test/measure directly the analog signals). Although the advantage of the physical quantification of the source of randomness in dedicated tests is undeniable, it can be difficult or even impossible to prove mathematically that the given tests are at least as effective as existing general-purpose continuous tests (as required by the standard).

Short bio:

Viktor Fischer received his M.S. and Ph.D. degrees in Electrical Engineering from Technical University of Kosice in Slovakia. From 1981 to 1991 he held an Assistant Professor position in the Department of Electronics of the Technical University of Kosice. From 1991 to 2006 he was a part-time invited professor at the University of Saint-Etienne, France. From 1999 to 2006 he was also a consultant with Micronic Slovakia, oriented in hardware data security systems. From 2006 he is a full-time Professor at the University of Saint-Etienne, France. His research interests include cryptographic engineering, secure embedded systems, cryptographic processors and especially true random number generators embedded in logic devices.